

DETAILED ACTION

1. This office action is response to the amendment filed on 10/01/2009. Claims 13, 16, 21-24 are amended. Claims 25-31 are newly added claims. Claims 13-31 are presented for examination.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's representative Linda Lecomte on March 11, 2010.

Amendment to the claims

13. (Currently Amended) A method for encrypting data according to an asymmetrical method using a processor, based on a factorization problem, comprising: having providing a public key to the processor; and providing a private key to the processor; wherein the public key includes being the iteration number L as well as the composite number n; n preferably being the product of a plurality of large prime numbers; the a private key is made up of the factorization of n; the a message $m = (m_1, m_2)$ to be encrypted is made

up of at least ~~the~~ components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$, c_1 and c_2 being integral numbers; $f(m) = (f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2=(m_1 \text{ op}_2 m_2) \bmod n$; ~~op_1 preferably being an addition and op_2 preferably being a multiplication~~; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thereby being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)_L$ wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a and b to obtain a set of roots and by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step.

Cancel claim 14.

Cancel claim 15.

21. (Currently Amended) A method for generating a signature using a processor, comprising:

wherein generating using the processor a signature is generated by interchanging the encryption and decryption steps, including functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key being the iteration number L as well as the includes a composite number n ; n preferably being the product of a plurality of large prime

~~numbers; the a~~ private key being made up of the factorization of n ; ~~the a~~ message $m = (m_1, m_2)$ to be encrypted is made up of at least ~~the~~ components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$; $f(m) = (f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2=(m_1 \text{ op}_2 m_2) \bmod n$; ~~op₁ preferably being an addition and op₂ preferably being a multiplication~~; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thereby being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$, c_1 and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 rood 4, can be communicated by 2 bits per iteration step.

Cancel claim 22.

23. (Currently Amended) A data carrier storage for a computer, comprising: storage of a software for the computer, the software being instructions configured to be executed by the computer, the instructions which, when executed by the computer, cause the performance of ~~comprising~~ functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key being the iteration number L as well as the includes a composite number n , n preferably being the product of a plurality of large prime

~~numbers; the a~~ private key being made up of the factorization of n ; ~~the a~~ message $m = (m_1, m_2)$ to be encrypted is made up of at least ~~the~~ components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$; $f(m) = (f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2=(m_1 \text{ op}_2 m_2) \bmod n$; ~~op₁ preferably being an addition and op₂ preferably being a multiplication~~; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thereby being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$, c_1 and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step.

24. (Currently Amended) A computer system, comprising-
a device that ~~allows the execution of~~ executes a method, the method having comprising:
software for a computer, comprising functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key being the iteration number L as well as the includes a composite number n , ~~n preferably being the product of a plurality of large prime numbers~~; the private key being made up of the factorization of n ; ~~the a~~ message $m = (m_1, m_2)$ to be encrypted is made up of at least ~~the~~ components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$; $f(m) = (f_1(m), f_2$

(m)) being applicable, and $f_1=(m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2=(m_1 \text{ op}_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thereby being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)_{\perp} c_1$, and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step.

Cancel claim 29.

Amendment to the specification

The following amended specification should be entered at page 1, after the Title ("ENCRYPTION METHOD BASED ON FACTORIZATION").

"SUMMARY OF THE INVENTION:

The present invention provides a method for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number L as well as the composite number n , n preferably being the product of a plurality of large prime numbers; the

private key is made up of the factorization of n ; the message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$; $f(m) = (f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2=(m_1 \text{ op}_2 m_2) \bmod n$; op_1 being, for example, an addition and op_2 being, for example, a multiplication. The encryption function $f(x)$ is selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thus being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$. In an embodiment, a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i . In an embodiment, the multivaluedness of the quadratic equation is eliminated by calculating a parity and a Jacobi symbol which, for example, in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step. In an embodiment, general iterations $f_1=(k_1 \cdot m_1 + k_2 \cdot m_2) \bmod n$ as well as $f_2= k_3 \cdot m_1 \cdot m_2 \bmod n$ are used, constants being part of the public key. In an embodiment, the composite number n as public key contains more than two factors. In an embodiment, the message is now made up of an N -tuple $m=(m_1 \dots m_n)$, the formula for the L th iteration step using dependencies of N values in each iteration step. In an embodiment, the multivaluedness is resolved by additional bits that are derived from the values obtained in each iteration. In an embodiment, the multivaluedness is resolved by redundancy in the transmitted data.

The present invention provides a method for generating a signature, wherein a signature is generated by interchanging the encryption and decryption steps from one or more of the method embodiments described herein. The present invention provides a software for a computer which implements one or more of the method embodiments described herein. That is, the software being instructions configured to be executed by the computer, the instructions which, when executed by the computer, cause the performance of one or more of the method embodiments described herein. the present invention provides for a data carrier for a computer, characterized by the storage of software for the computer which implements one or more of the method embodiments described herein.

DETAIL DESCRIPTION"

Response to Arguments

Applicant's arguments filed on 10/01/2009 have been fully considered and they are persuasive.

Allowable Subject Matter

3. **Claims 13, 16-21, 23-28 and 30-31** are allowed in light of the Applicant's argument and in light of the prior art made of record.

Reasons for Allowance

4. The following is a statement of reasons for allowance: As to independent claims 13, 21, 23 and 24, the prior art of record (US Publication No. Patent No. 6266411, Patent No. 6052467 and "An Identity Based Encryption Scheme Based on Quadratic Residues") alone or in combination fails to anticipate or render obvious the claim invention wherein the novel features includes,

Etzel et al. (prior art on the record) teaches the first input transformed message is processed by a first iteration of a CMEA process using the first CMEA key to produce a first intermediate ciphertext. This first intermediate ciphertext is subjected to a first output transformation to produce a first output transformed message. The first output transformed message is subjected to a second input transformation to produce a second input transformed message. Brands (prior art on the record) teaches the composite number n is a product of two distinct prime numbers p and q . The secret key is the prime factorization of n . Brands further teaches to construct efficient and secure restrictive blind certificate issuing protocols, by means of which an issuer party can issue triples consisting of a secret key, a matching public key and a corresponding certificate, such that the public key and the certificate can be perfectly blinded by the receiving party. Cocks (prior art on the record) teaches the system generates a universally available public modulus M . This modulus is a product of two primes P and Q . Further, Cocks teaches a square modulo both P and Q , and hence is a square

modulo M , or else $-a$ is a square modulo P , Q and hence M . either a or $-a$ will be quadratic residues modulo P and Q where the authority can calculate the square root modulo M and send it to Alice. Alice decrypted message s by calculating Jacobi symbol to recover original message.

None of the prior art of record teaches the novel feature of the present invention as the public key being the iteration number L as well as the composite number n , n preferably being the product of a plurality of large prime numbers; the private key is made up of the factorization of n ; the message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 and m_2 ; an encryption function $f(x)$ is iterated a total of L times, with $c = (c_1, c_2) = f^L(m)$; $f(m) = (f_1(m), f_2(m))$ being applicable, and $f_1 = (m_1 \text{ op}_1 m_2) \bmod n$ as well as $f_2 = (m_1 \text{ op}_2 m_2) \bmod n$; op_1 being, for example, an addition and op_2 being, for example, a multiplication. The encryption function $f(x)$ is selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thus being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$ wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form $3 \bmod 4$, can be communicated by 2 bits per iteration step.

The present invention provides a method for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number L as well as the composite number n , n preferably being the product of a plurality of large prime numbers. The

encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L -fold solution of a quadratic equation modulo n , it thereby being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$ where a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol to improve redundancy in the transmitting data.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Therefore, **13, 16-21, 23-28 and 30-31** are hereby allowed in view of applicant's persuasive arguments and in the light of amendments to the claims.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see form "PTO-892 Notice of Reference Cited").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MORSHED MEHEDI whose telephone number is (571) 270-7640. The examiner can normally be reached on M - F, 8:00 am to 5:00 pm EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Taghi T Arani can be reach on (571) 272-3787. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from their Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (In USA or Canada) or 571-272-1000.

/M. M./
Examiner, Art Unit 2438
/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438